Abstract

A system for network security transparently occupies an observation port on the data stream, passing the entire range of network information to a dedicated interpreter. The interpreter resolves the data stream into individual data packets, which are then assembled into reconstructed network sessions according to parameters such as protocol type, source and destination addresses, source and destination ports, sequence numbers and other variables. The different types of sessions may include the traffic of many different types of users, such as e-mail, streaming video, voice-over-Internet and others. The system detects and stores the sessions into a database. A parser module may extract only the minimum information needed to reconstruct individual sessions. A backend interface permits a systems administrator to interrogate the forensic record of the network for maintenance, security and other purposes. The invention is not constrained to detect limited types of data, but rather captures and records a comprehensive record of network behavior.